Patch Release Note

Patch 86222-14 For Rapier Switches and AR800 Series Modular Switching Routers

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86222-14 for Software Release 2.2.2 on existing models of Rapier L3 managed switches and AR800 Series L3 modular switching routers. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86222-14.

Base Software Release File	86s-222.rez
Patch Release Date	28-Feb-2002
Compressed Patch File Name	86222-14.paz
Compressed Patch File Size	335336 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.2.2 for Rapier Switches, AR300 and AR700 Series Routers, and AR800 Series Modular Switching Routers (Document Number C613-10313-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Switch Documentation Set for Software Release 2.2.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AR800 Series Modular Switching Router Documentation Set for Software Release 2.2.1 available on the Documentation and Tools CD-ROM packaged with your switching router, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Features in 86222-14

Patch 86222-14 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02005 Module: IPG Network affecting: No

When telnetting to the switch, the TCP connection was reset, and when the packet was passed to IPG_Forward a fatal error occurred. This patch implements a workaround.

PCR: 02035 Module: VLAN Network affecting: No

The CREATE CONFIG command now correctly configures tagged ports belonging to VLANs not in the default STP.

PCR: 02036 Module: SWITCH Network affecting: No

A new command allows the Layer 3 aging timer to be changed:

SET SWITCH L3AGEINGTIMER=<seconds>

where seconds can be 30 - 43200. After each cycle of the ageing timer, all existing Layer 3 entries with the hit bit set will have the hit bit reset to zero, and all existing Layer 3 entries with the hit bit set to zero will be deleted.

The SHOW SWITCH command output now displays the Layer 3 ageing timer value.

PCR: 02038 Module: PING Network affecting: No

Resolution of PCR 02011 in Patch 12 sometimes caused a fatal error. This issue has been resolved.

PCR: 02039 Module: IPG Network affecting: No

The SHOW IP ROUTE FILTER command output displayed counters for 'passes' and 'include' that were the same. This issue has been resolved. Counters now increment only when a filter is active and do not count interface routes.

PCR: 02040 Module: SWI Network affecting: No

PCR 02019 permitted the reception of packets by the CPU that should have been discarded. This issue has been resolved.

PCR: 02057 Module: FIREWALL Network affecting: No

Firewall TCP timeout values have been reduced for sessions placed in the CLOSED state after receiving a TCP/RESET. This applies to the stateful inspection of firewall sessions only, and not to the TCP module. Previously, PCR 01263 reduced the timeout value for sessions placed in the CLOSED state after a TCP/FIN packet was received.

PCR: 02063 Module: FIREWALL Network affecting: No

Firewall IP access lists were not working correctly. If an IP range was specified without spaces between the IP address and the separating '-' the range would be ignored. Spaces are no longer required. Also, matches were made to addresses covered by a range in an access list if the matching range was numerically the lowest in the list. This issue has been resolved.

Features in 86222-13

Patch file details for Patch 86222-13 are listed in Table 3.

Table 2: Patch file details for Patch 86222-13.

Base Software Release File	86s-222.rez
Patch Release Date	1-Feb-2002
Compressed Patch File Name	86222-13.paz
Compressed Patch File Size	328884 bytes

Patch 86222-13 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 02014 Module: TELNET Network affecting: No

When a Telnet session was terminated without a proper logout, counters recording the number of logins were not correctly decremented. This issue has been resolved.

PCR: 02019 Module: SWI Network affecting: No

If a layer 3 hardware filter for a particular packet type (e.g. Netbeui) was configured, all IP packets destined for the CPU were discarded. This issue has been resolved.

Features in 86222-12

Patch file details for Patch 86222-12 are listed in Table 3.

Table 3: Patch file details for Patch 86222-12.

Base Software Release File	86s-222.rez
Patch Release Date	18-Jan-2001
Compressed Patch File Name	86222-12.paz
Compressed Patch File Size	328528 bytes

Patch 86222-12 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01223 Module: IPG Network affecting: No

If route filters existed and a RESET IP command was executed, some static and interface routes were incorrectly removed if the filters matched. This issue has been resolved.

PCR: 01257 Module: DHCP Network affecting: No

DHCP occasionally caused a fatal error. Also, while an address was in the reclaiming list, a DHCPDISCOVERY message requesting the address made the address disappear. These issues have been resolved.

PCR: 01261 Module: IPG/VRRP Network affecting: No

A fatal error occurred when forwarding IP packets with VRRP enabled. This issue has been resolved.

PCR: 01263 Module: FIREWALL Network affecting: No

The firewall TCP timeout values for sessions in the CLOSED and TIMEWAIT states have been reduced. This only applies to the stateful inspection of firewall sessions and not to the TCP module.

PCR: 01268 Module: SWI Network affecting: No

When a Rapier was under heavy load from software routing (e.g. after a reboot and before the routing tables were refreshed), OSPF could take a long time to converge. This patch gives OSPF packets higher priority to expedite OSPF convergence.

PCR: 01269 Module: SWI Network affecting: No

A new feature permits hardware filtering by the Rapier family based on the Ethernet frame type. The TYPE parameter:

```
TYPE={802|ETHII|SNAP}
```

has been added to the following commands:

ADD SWITCH L3FILTER ENTRY

ADD SWITCH L3FILTER MATCH

SET SWITCH L3FILTER ENTRY

SET SWITCH L3FILTER MATCH

SHOW SWITCH L3FILTER

PCR: 01272 Module: SWI Network affecting: No

A physical port could not be re-enabled once disabled when STP was active. This issue has been resolved.

PCR: 01273 Module: SWI Network affecting: No

The CREATE CONFIG command now includes the STPFORWARDING parameter in generated scripts. The SHOW SWITCH command now displays the setting of STPFORWARDING.

PCR: 01274 Module: SWI Network affecting: No

Refinements were made to the switch chip register settings improving CoS provision with the newer revision of switching silicon on the Rapier 16, Rapier 24 and Rapier 48.

PCR: 01275 Module: FIREWALL Network affecting: No

The firewall was incorrectly forwarding multicast packets originating from a private address in cases where a matching route was defined. This issue has been resolved.

PCR: 01276 Module: SWI Network affecting: No

When the speed of one or more switch ports was forced to a half duplex setting and the ports were then added to a trunk group configured for full duplex operation, the port settings were not overridden by the trunk group speed setting. The trunk group speed setting will now take precedence over the port speed setting.

PCR: 01287 Module: OSPF Network affecting: No

Configuring IP route filters did not stop flooding of AS external LSAs to neigbours at startup. The result was that the neigbour received the AS LSAs and added the corresponding routes into its own routing table. However, after some time (e.g. 1 hour), the AS external LSAs in the neigbour's database disappeared, but the corresponding routes were still in its routing table. This issue has been resolved.

PCR: 01289 Module: VRRP Network affecting: No

The checksum in VRRP advertisements was not being calculated correctly. The calculation was not compatible with the RFC. This issue has been resolved.

PCR: 01290 Module: PPP Network affecting: No

When PPP was running over Ethernet to a client from another vendor, the Maximum Transmission Unit value for the link was not adjusted from the PPP default of 1500 to 1492. This issue has been resolved.

PCR: 01291 Module: IPG(IGMP) Network affecting: No

IGMP did not send the Start Up Query, and the Other Querier Present Timer did not change the Time Out value accordingly if Query Interval was changed. IGMP did not notify other registered parties (PIM and DVMRP) when a port was deleted from a membership group. IGMP reported a membership leave to other parties while it was still waiting for a reply to a group specific query from a leaving member. These issues have been resolved.

PCR: 02003 Module: FIREWALL Network affecting: No

The timeout value for ICMP session entries in the firewall can now be adjusted via the OTHERTIMEOUT parameter of the SET FIRE POLICY command. Note: if the value for OTHERTIMEOUT is set to more than 10 minutes the timeout used for ICMP sessions will default to 10 minutes.

PCR: 02007 Module: DHCP Network affecting: No

When a DHCP server received a DHCP DISCOVERY packet passed by a relay agent, requesting an IP address that did not belong to the subnet the client and the relay agent were attached to, it offered the requested address if it was available. The DHCP server will now only offer an IP address from the subnet that connects the client and the relay agent.

PCR: 02008 Module: TRIGGER Network affecting: No

The first periodic after day trigger boundary (i.e. midnight) did not occur. A range check error occurred due to an incorrect comparison. These issues have been resolved.

PCR: 02011 Module: PING Network affecting: No

Stopping a trace route using STOP TRACE occasionally caused a fatal error. This issue has been resolved.

PCR: 02012 Module: IPG, VLAN, SWI Network affecting: No

IGMP reflooded packets with VLAN tagging were not processed correctly. This issue has been resolved.

Features in 86222-11

Patch file details for Patch 86222-11 are listed in Table 4.

Table 4: Patch file details for Patch 86222-11.

Base Software Release File	86s-222.rez
Patch Release Date	19-Dec-2001
Compressed Patch File Name	86222-11.paz
Compressed Patch File Size	296244 bytes

Patch 86222-11 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01243 Module: SWI Network affecting: No

When a Rapier CPU was handling a large amount of traffic and a busy egress port went down, it was possible for the transmission of packets by the CPU to cease. This issue has been resolved.

PCR: 01265 Module: SWI Network affecting: No

When trunking was in operation, in some instances the switch transmitted tagged packets on untagged trunk ports. This issue has been resolved.

PCR: 01288 Module: SWI Network affecting: No

When a switch port was forced to half duplex mode and the link partner was forced to full duplex mode, it was possible for the switch to enter a state where it was unable to transmit packets. This issue has been resolved.

Features in 86222-10

Patch file details for Patch 86222-10 are listed in Table 5.

Table 5: Patch file details for Patch 86222-10.

Base Software Release File	86s-222.rez
Patch Release Date	29-Nov-2001
Compressed Patch File Name	86222-10.paz
Compressed Patch File Size	295536 bytes

Patch 86222-10 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancement:

PCR: 01264 Module: SWI Network affecting: No

Some switch chip register settings have been optimised to improve the provision of CoS with the newer revision of switching silicon.

Features in 86222-09

Patch file details for Patch 86222-09 are listed in Table 6.

Table 6: Patch file details for Patch 86222-09.

Base Software Release File	86s-222.rez
Patch Release Date	27-Nov-2001
Compressed Patch File Name	86222-09.paz
Compressed Patch File Size	295444 bytes

Patch 86222-09 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01189 Module: STP, SWI Network affecting: Yes

A new feature, STP forwarding, has been added. STP forwarding can be enabled and disabled using the commands:

```
ENABLE SWI STPFORWARD
DISABLE SWI STPFORWARD
```

When STP forwarding is enabled, all STP forwarding is ignored and all BDPUs received on a port are forwarded on all other ports.

PCR: 01242 Module: CORE, SNMP Network affecting: No

The switch now delays sending link traps immediately after a restart to give the link to the trap host time to come up. A similar change has been made for the cold start trap. After a 10s delay, all interfaces which are UP have a link trap generated for them. After that, link traps are sent as normal.

PCR: 01244 Module: SWI, CORE, IPG Network affecting: No

Processing invalid UDP packets caused a memory leak. This issue has been resolved. Additional debugging facilities were added.

PCR: 01246 Module: SWI Network affecting: No

The default setting for the switch port parameter INFILTERING is now OFF, as specified in IEEE802.1Q. A VLAN will still reject these packets if they are not from valid VLAN member ports.

PCR: 01247 Module: IPG Network affecting: No

The IGMP snooping forwarding process now correctly selects outgoing ports when DVMRP is managing the multicast routing information.

PCR: 01248 Module: SWI Network affecting: No

A configuration problem prevented trunking of gigabit ports at 100Mbit speeds. This issue has been resolved. The A39 gigabit copper uplink reverted to autonegotiation after a restart, even if it was configured to a fixed speed. This issue has been resolved. When the port has been configured for a fixed speed, the mode is now set to MDIX, not MDI.

PCR: 01254 Module: PRI Network affecting: No

When an M2 version of the AR020 PRI E1/T1 PIC was installed in a AR040 NSM it was not possible to select the T1 mode of operation regardless of the jumper setting. This issue has been resolved.

PCR: 01256 Module: Firewall Network affecting: No

A fatal error occurred when the firewall discarded disallowed multicast packets. This issue has been resolved.

Features in 86222-08

Patch file details for Patch 86222-08 are listed in Table 7.

Table 7: Patch file details for Patch 86222-08.

Base Software Release File	86s-222.rez
Patch Release Date	09-Nov-2001
Compressed Patch File Name	86222-08.paz
Compressed Patch File Size	291012 bytes

Patch 86222-08 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01201 Module: L2TP Network affecting: Yes

Tunnel creation failed when attempting to establish a point-to-point tunnel from an ATR router (tunnel originator) to another vendor's router. This issue has been resolved.

PCR: 01233 Module: PIM Network affecting: No

When IGMP snooping was enabled, if a member left a group on a port, it could not re-join the group on that port. This issue has been resolved.

Substantial changes have been made to PIM in more recent code releases. These have been retrofitted to 2-2-2 in the patch. Note: these changes have incorporated PCRs 01159 and 01190.

PCR: 01236 Module: PPP Network affecting: No

The PPPoE access concentrator did not stop RADIUS accounting when a PADT termination was received without receiving a proper PPP termination first. This issue has been resolved.

PCR: 01237 Module: SWI Network affecting: No

The dot1dBridge MIB implementation now complies with RFC1493.

Features in 86222-07

Patch file details for Patch 86222-07 are listed in Table 8:

Table 8: Patch file details for Patch 86222-07

Base Software Release File	86s-222.rez
Patch Release Date	26-Oct-2001
Compressed Patch File Name	86222-07.paz
Compressed Patch File Size	250468 bytes

Patch 86222-07 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01018 Module: DHCP Network affecting: No

DHCP now correctly handles request messages containing request list options not supported by the router.

PCR: 01160 Module: IPG,FIREWALL Network affecting: No

The router would accept TCP sessions with destination address the same as the subnet broadcast address for one of the router's interfaces. Firewall-generated packets destined for a subnet broadcast address on one of the routers interfaces would cause a fatal error. These issues have been resolved.

PCR: 01168 Module: HTTP Network affecting: No

A watchdog timout occurred when the router received an HTTP message with an over-length header. Normal HTTP requests would also occasionally cause watchdog timeouts. These issues have been resolved.

PCR: 01182 Module: OSPF Network affecting: No

The OSPF route filter was not filtering out external routes. This issue has been resolved.

PCR: 01193 Module: IPG Network affecting: No

MD5 Authentication now works correctly with RIP packets.

PCR: 01194 Module: L2TP, IPG Network affecting: No

The SET IP LOCAL command caused a fatal error if the router was configured with a default route over an L2TP tunnel, because there was no valid route to the remote IP address of the tunnel. This issue has been resolved.

PCR: 01197 Module: Q931 Network affecting: No

Debug messages are no longer generated when a Q.931 Advise of Charge Notification message is received.

PCR: 01198 Module: TCP Network affecting: No

TCP sessions would get stuck in the FINWAIT2 state if the remote host did not send a FIN message when required. The router now starts a timer when a TCP session enters the FINWAIT2 state and will automatically close the session if the timer expires.

PCR: 01199 Module: IPG Network affecting: No

The SET IP FILTER command was not correctly handling the ICMPTYPE and ICMPCODE parameters. This issue has been resolved.

PCR: 01202 Module: DHCP Network affecting: No

The router will now accept DHCP messages that are greater than or equal to 576 bytes in size, and reject any message smaller than 576 bytes. This operation conforms to RFC 1541.

PCR: 01203 Module: ISAKMP Network affecting: No

ISAKMP quick mode exchanges are now committed if any traffic is received over the newly generated SA. This improves stability in very lossy networks where the commit message may get lost.

PCR: 01204 Module: ISAKMP Network affecting: No

ISAKMP debugging caused a fatal error when the debugging mode was set to ALL and PFS was enabled. This issue has been resolved.

PCR: 01205 Module: PPP Network affecting: No

PPPoE interfaces with IDLE set to ON would not retry active discovery when more data was received if active discovery had previously failed. This issue has been resolved.

PCR: 01206 Module: ISAKMP Network affecting: No

A memory loss occurred when certificates were used by ISAKMP. This issue has been resolved.

PCR: 01207 Module: ISAKMP Network affecting: No

ISAKMP heartbeats are no longer transmitted if the lower layer interface is down. This stops ISAKMP heartbeats from bringing up links in dial-up environments.

PCR: 01209 Module: ISAKMP Network affecting: No

In some conditions it was possible for ISAKMP packets to be lost and not retransmitted. Incoming ISAKMP messages are now validated before stopping retransmission of the previous message.

PCR: 01211 Module: SWI Network affecting: No

The COS_DST bit on ARL for L3 interface should be 0x4 (higher priority) for CPU ports. This has been corrected.

PCR: 01213 Module: TRG, SNMP Network affecting: No

The Trigger Facility was generating a trap with variable { 0 0 }, and was not documented in the ATI enterprise MIB. This issue has been resolved. The MIB object *triggerLastTriggerActivated* ({ enterprises(1) alliedTelesyn(207) mibObjects(8) brouterMib(4) atrouter(4) modules(4) trigger(53) 1 }) has been

defined, to record the trigger number of the last trigger activated, and this variable is now transmitted in the trigger activation trap *triggerTrap*.

PCR: 01214 Module: SWI Network affecting: No

In a Rapier G6, fitted with a fibre uplink module with all ports active, switching traffic between port 1 and the uplink caused the traffic flow to cease after a period of time depending on the volume of traffic. This issue has been resolved.

PCR: 01216 Module: STP Network affecting: No

The Rapier did not include the message age of the received BDPU message in the message age of the BDPU it transmitted. Also, the message age of the message transmitted BDPU could be less than that of the received BDPU, which contravenes IEEE 802.3d. This issue has been resolved.

PCR: 01219 Module: VLAN,SWI Network affecting: No

Reception of incorrectly tagged packets was causing corruption of the ARL table, eventually causing the switch to lock up. This issue has been resolved. Tagged packets with invalid VLAN identifiers are now discarded. The INFILTERING parameter of the SET SWITCH PORT command now defaults to ON.

PCR: 01221 Module: SWI Network affecting: No

Flow control performance has been improved.

PCR: 01225 Module: IPSEC Network affecting: No

The IPsec SA ID now wraps correctly at the 16 bit (ID = 65535) boundary. The ID is also checked to verify that it is free before it is used.

PCR: 01227 Module: PPP Network affecting: No

If PPPoE AC services were not deleted in the same order they were added, the DELETE command would return an " operation successful" message but the service would still appear in the output of the SHOW PPP PPPOE command. This issued has been resolved.

PCR: 01229 Module: SWI Network affecting: No

The CREATE CONFIG command did not include all required L3FILTER parameters in the generated script file.

PCR: 01232 Module: SWI Network affecting: No

The L3 table on the Rapier G6 is now cleared when a switch port goes down to ensure the L3 and ARP tables are consistent.

PCR: 01234 Module: SWI Network affecting: No

A switch port that was transmitting STP BPDUs and also mirroring its transmit traffic to the mirror port caused a fatal error. This issue has been resolved.

Features in 86222-06

Patch file details for Patch 86222-06 are listed in Table 9.

Table 9: Patch file details for Patch 86222-06.

Base Software Release File	86s-222.rez
Patch Release Date	30-Aug-2001
Compressed Patch File Name	86222-06.paz
Compressed Patch File Size	226776 bytes

Patch 86222-06 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01188 Module: SWI Network affecting: No

The power supply voltages of the base board PHYs on a Rapier G6 are controlled by a PHY register value, which was incorrectly set. This issue has been resolved.

PCR: 01190 Module: PIM Network affecting: No

In PIM Dense Mode, if a data stream started before PIM hello messages were exchanged, the receiver did not get the data stream. This issue has been resolved.

PCR: 01192 Module: SWI Network affecting: No

The Rapier G6 base ports sometimes experienced spurious link up or link down events. This issue has been resolved.

Features in 86222-05

Patch file details for Patch 86222-05 are listed in Table 10.

Table 10: Patch file details for Patch 86222-05.

Base Software Release File	86s-222.rez
Patch Release Date	24-Aug-2001
Compressed Patch File Name	86222-05.paz
Compressed Patch File Size	223728 bytes

Patch 86222-05 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01148 Module: SWI Network affecting: No

A39 copper uplink modules in the Rapier G6 sometimes experienced spurious link up or link down events. This issue has been resolved.

PCR: 01157 Module: CORE Network affecting: No

The enterprise MIB now supports objects for power supply monitoring.

PCR: 01162 Module: PKI Network affecting: No

Certificates containing *GeneralisedTime* with the year in YYYY format are now parsed correctly. The *keyUsage* field of certificates is now parsed correctly when only one byte has been specified. The *CRL update time* is now displayed correctly in hours. If the *username* and *password* parameters are present the *location* parameter must be present and appear before the *username* and *password* parameters. Certificates with signatures of 257 bytes are now correctly parsed. Certificates added from a configuration script are now processed correctly.

PCR: 01170 Module: IPv6 Network affecting: No

A fatal error occurred if an IPv6 interface was deleted while packets were being transmitted. The number of current interfaces was not being updated correctly when a new IPv6 interface was added. As a result, after multiple additions and deletions, no more IPv6 interfaces could be added. These issues have been resolved.

PCR: 01176 Module: PKI Network affecting: No

The CREATE CONFIG command now adds PKI certificates to the script in the same order that they were originally added to the certificate database.

PCR: 01177 Module: PKI Network affecting: No

PKI certificates are now periodically checked (once per hour) to verify that they are still valid.

PCR: 01178 Module: IPSEC Network affecting: No

IPCOMP SA's which have the reserved CPI "3" are no longer deleted by ISAKMP delete messages.

PCR: 01179 Module: SWI Network affecting: No

When a VLAN was created and then destroyed on the G6 or G6F, the VTABLE was corrupted. This has been fixed.

PCR: 01181 Module: DHCP Network affecting: No

DHCP failed to send request messages when it was in a rebinding or renewing state. This issue has been resolved.

PCR: 01185 Module: SWI Network affecting: No

In some extreme traffic conditions the switch could lock up, preventing switching of any traffic. This issue has been resolved.

PCR: 01186 Module: FIREWALL Network affecting: No

When large numbers of sessions were being handled the firewall would become overly aggressive in restricting new sessions. The *Active TCP Opens* field in the output of the SHOW FIREWALL POLICY would show a very high number (42×10^8). This issue has been resolved.

PCR: 01187 Module: IPG Network affecting: No

If the IGMP table was empty and a timeout was set, a fatal error occurred. This issue has been resolved.

Features in 86222-04

Patch file details for Patch 86222-04 are listed in Table 11.

Table 11: Patch file details for Patch 86222-04.

Base Software Release File	86s-222.rez
Patch Release Date	24-Aug-2001
Compressed Patch File Name	86222-04.paz
Compressed Patch File Size	220220 bytes

Patch 86222-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01124 Module: PKI Network affecting: No

Message protection validation failures would occur intermittently. This issue has been resolved.

PCR: 01136 Module: ISAKMP Network affecting: No

ISAKMP now interoperates with other vendor's products in aggressive mode exchanges.

PCR 01138 Module: CORE, SWI Network affecting: No

Support has been added for the 8624XL-80 switch with -48VDC power supply.

PCR: 01152 Module: FIREWALL Network affecting: No

In a dual policy configuration, the firewall would lock up under load. The firewall would also mistakenly report SYN attacks. These issues have been resolved.

PCR: 01159 Module: PIM Network affecting: No

The CREATE CONFIG command generated duplicate PIM interface configuration command lines. This issue has been resolved.

PCR: 01162 Module: PKI Network affecting: No

Certificates containing *GeneralisedTime* with the year in YYYY format are now parsed correctly. The *keyUsage* field of certificates is now parsed correctly when only one byte has been specified. The *CRL update time* is now displayed correctly in hours. If the *username* and *password* parameters are present the *location* parameter must be present and appear before the *username* and *password* parameters.

PCR: 01165 Module: DHCP Network affecting: No

The DHCP server now correctly allocates addresses to clients running Apple Open Transport 2.5.1 or 2.5.2.

PCR: 01166 Module: FIREWALL Network affecting: No

Both public and private access could be configured on the same interface on a policy. This issue has been resolved.

PCR: 01167 Module: ENCO Network affecting: No

RSA encryption is now periodically suspended to ensure other processes get some CPU time during large RSA calculations.

PCR: 01169 Module: ISAKMP Network affecting: No

The CREATE ISAKMP command now checks that the key specified by the LOCALRSAKEY parameter actually exists in the ENCO module.

PCR: 01171 Module: ETH, TRIGGER Network affecting: No

The INTERFACE parameter of the CREATE TRIGGER and SET TRIGGER commands now supports Ethernet interfaces. Ethernet interface events can now generate triggers.

PCR: 01173 Module: Telnet Network affecting: No

The Telnet server's listen port can now be configured to a number in the range 1 to 65535, excluding any ports already assigned as listen ports.

PCR: 01174 Module: Firewall Network affecting: No

The CREATE CONFIG command sometimes generated scripts for rule commands with GBLIP=0.0.0.0 when this was not necessary. This issue has been resolved.

Features in 86222-03

Patch file details for Patch 86222-03 are listed in Table 12.

Table 12: Patch file details for Patch 86222-03.

Base Software Release File	86s-222.rez
Patch Release Date	8-Aug-2001
Compressed Patch File Name	86222-03.paz
Compressed Patch File Size	205828 bytes

Patch 86222-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01112 Module: IPG Network affecting: No

DNS response packets with corrupt length fields were causing a fatal error. This issue has been resolved.

PCR: 01139 Module: IPG Network Affecting: No

IP NAT caused a fatal error when an ARP wait timer timed out and tried to send a host unreachable message. This issue has been resolved.

PCR: 01147 Module: STT Network affecting: No

The router was restarting after a "teardrop" attack on the STT listen port. This issue has been resolved.

PCR: 01150 Module: FIREWALL Network affecting: No

The entry aging process now works correctly even when there are large numbers of firewall entries to be aged.

PCR: 01153 Module: IPG Network affecting: No

The command SHOW IP DEBUG=*n* was entered, where *n* was one greater than the number of items in the IP debug queue resulted in a fatal error. This issue has been resolved.

Features in 86222-02

Patch file details for Patch 86222-02 are listed in Table 13.

Table 13: Patch file details for Patch 86222-06.

Base Software Release File	86s-222.rez
Patch Release Date	26-Jul-2001
Compressed Patch File Name	86222-02.paz
Compressed Patch File Size	202564 bytes

Patch 86222-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.2.2, and the following enhancements:

PCR: 01081 Module: FIREWALL Network affecting: No

When an interface on the firewall was configured with a global IP address of 0.0.0.0, outgoing packets from the private interface to the public interface sometimes caused a fatal error. This issue has been resolved.

PCR: 01126 Module: PKI Network affecting: No

Re-validation of temporary CA certificates now works correctly.

PCR: 01128 Module: IPG Network affecting: No

A fatal error occurred when IGMP received a *Join* message and attempted to forward the *Join* message to other switch ports. This issue has been resolved.

PCR: 01131 Module: CORE Network affecting: No

The SHOW CPU command sometimes displayed incorrect CPU utilisation figures. Typically a value of about 74% was reported when in fact the CPU was almost idle. This issue has been resolved.

PCR: 01134 Module: GUI Network affecting: No

Port parameters can now be set correctly using the Layer 3 Switch GUI.

PCR: 01135 Module: GUI,INST Network affecting: No

Clicking the *Apply* button on a Layer 3 Switch GUI page caused the switch to lock up if no configuration file was set, but boot.cfg was present. This issue has been resolved.

PCR: 01137 Module: IPG Network affecting: No

A fatal error occurred when UDP received a packet with very long UDP packet length. This issue has been resolved.

Features in 86222-01

Patch file details for Patch 86222-01 are listed in Table 14.

Table 14: Patch file details for Patch 86222-01.

Base Software Release File	86s-222.rez
Patch Release Date	11-Jul-2001
Compressed Patch File Name	86222-01.paz
Compressed Patch File Size	187124 bytes

Patch 86222-01 includes the following enhancement for Software Release 2.2.2:

PCR: 01100 Module: DHCP Network affecting: No

The DHCP server identified the wrong port numbers for incoming DHCP requests causing DHCP replies to be sent to the wrong port. This issued has been resolved.

PCR: 01102 Module: IPG Network affecting: No

The IP flow cache occasionally generated a watchdog fatal error. This issued has been resolved.

PCR: 01102 Module: SWI Network affecting: No

Deleting entries from an L3 table occasionally resulted in a watchdog fatal error. This issued has been resolved.

PCR: 01106 Module: PKI Network affecting: No

PKI enrolment no longer causes message validation to fail.

PCR: 01119 Module: IPV6 Network affecting: No

Repeated addition and deletion of an address with the VALID parameter set to or from an IPV6 interface caused a fatal error. This issue has been corrected. The VALID parameter specifies the life of the address, and defaults to INFINITE. The address is deleted when the lifetime expires. The PREF parameter specifies the time that the address is the preferred address of the interface, and defaults to INFINITE. PREF must be less than or equal to VALID. IPV6 now checks and ensures that if either PREF or VALID is specified, PREF is less than or equal to VALID. When an address is deleted the timers are now correctly cleared.

PCR: 01120 Module: IPG Network affecting: No

IP sometimes passed the wrong port number to PIM, causing PIM to process the wrong port number in its routing table. This issued has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.